**A Vehicle Location Monitoring System for Wireless Sensor Networks**

**Abstract:-**

Monitoring personal locations with a potentially untrusted server poses privacy threats to the monitored individuals. To this end, we propose a privacy-preserving location monitoring system for wireless sensor networks. In our system, we design two innetwork location anonymization algorithms, namely, resource- and quality-aware algorithms, that aim to enable the system to provide high quality location monitoring services for system users, while preserving personal location privacy. Both algorithms rely on the well established k-anonymity privacy concept, that is, a person is indistinguishable among k persons, to enable trusted sensor nodes to provide the aggregate location information of monitored persons for our system. Each aggregate location is in a form of a monitored area A along with the number of monitored persons residing in A, where A contains at least k persons. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to maximize the accuracy of the aggregate locations by minimizing their monitored areas. To utilize the aggregate location information to provide location monitoring services, we use a spatial histogram approach that estimates the distribution of the monitored persons based on the gathered aggregate location information. Then the estimated distribution is used to provide location monitoring services through answering range queries.

We evaluate our system through simulated experiments. The results show that our system provides high quality location monitoring services for system users and guarantees the location privacy of the monitored persons.

**System Architecture:**



**Algorithm:**

The Resource-Aware Algorithm

**Existing System:**

Existing location monitoring systems. In an identity-sensor location monitoring System, since each sensor node reports the exact location information of each 0monitored object to the server, the adversary can pinpoint each object's exact location. On the other hand, in a counting-sensor location monitoring system, each sensor node reports the number of objects in its sensing area to the server. The adversary can map the monitored areas of the sensor nodes to the system layout. If the object count of a monitored area is very small or equal to one.

**Proposed System:**

This paper proposes a privacy-preserving location monitoring system for wireless sensor networks to provide monitoring services. Our system relies on the well established k-anonymity privacy concept, which requires each person is indistinguishable among k persons. In our system, each sensor node blurs its sensing area into a cloaked area, in which at least k persons are residing. Each sensor node reports only aggregate location information, We propose two in-network aggregate location anonymization algorithms, namely, resource- and quality-aware algorithms. Both algorithms require the sensor nodes to collaborate with each other to blur their sensing areas into cloaked areas, such that each cloaked area contains at least k persons to constitute a k-anonymous cloaked area. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to minimize the size of the cloaked areas, in order to maximize the accuracy of the aggregate locations reported to the server.

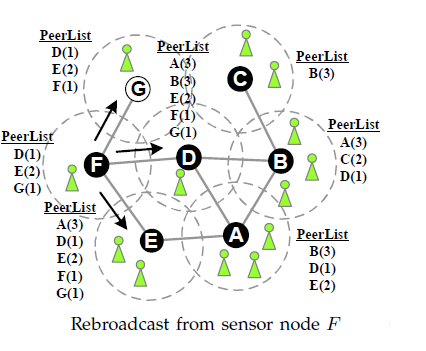
**Modules:**

**1. WSN Location Monitoring Module**

The location monitoring system using identity sensors, the sensor nodes report the exact location information of the monitored persons to the server; thus using identity sensors immediately poses a major privacy breach. To tackle such a privacy breach, the concept of aggregate location information, that is, a collection of location data relating to a group or category of persons from which individual identities have been removed , has been suggested as an effective approach to preserve location privacy .Although the counting sensors by nature provide aggregate location information, they would also pose privacy breaches.

**2. Aggregate locations Module**

We design two in-network location anonymization algorithms, namely, resource- and quality-aware algorithms that preserve personal location privacy, while enabling the system to provide location monitoring services. Both algorithms rely on the well established k-anonymity privacy concept that requires a person is indistinguishable among k persons. In our system, sensor nodes execute our location anonymization algorithms to provide k- anonymous aggregate locations, in which each aggregate location is a cloaked area A



**3. Mapped Location monitoring Module:**

**Sensor nodes**:

Each sensor node is responsible for determining the number of objects in its sensing area, blurring its sensing area into a cloaked area A, which includes at least k objects, and reporting A with the number of objects located in A as aggregate location information to the server. We do not have any assumption about the network topology, as our system only requires a communication path from each sensor node to the server through a distributed tree . Each sensor node is also aware of its location and sensing area.

**Server:**

The server is responsible for collecting the aggregate locations reported from the sensor nodes, using a spatial histogram to estimate the distribution of the monitored objects, and answering range queries based on the estimated object distribution. Furthermore, the administrator can change the anonymized level k of the system at anytime by disseminating a message with a new value of k to all the sensor nodes.

**System users:**

Authenticated administrators and users can issue range queries to our system through either the server or the sensor nodes, as depicted in Above System Architecture figure. The server uses the spatial histogram to answer their queries.

**4. Minimum bounding rectangle (MBR)**

****

We find the minimum bounding rectangle (MBR) of the sensing area of A. It is important to note that the sensing area can be in any polygon or irregular shape.

# Software Requirements:

**Hardware Requirement:**

Minimum 1.1 GHz PROCESSOR should be on the computer.

128 MB RAM.

20 GB HDD.

1.44 MB FDD.

52x CD-ROM Drive.

MONITORS at 800x600 minimum resolution at 256 colors minimum.

I/O, One or two button mouse and standard 101-key keyboard.

**Software Requirement:**

Operating System : Windows 95/98/2000/NT4.0.

Technology : JAVA, JFC(Swing)

Development IDE : Eclipse 3.x